

## Exhibit F

# Internet Control Message Protocol

From Wikipedia, the free encyclopedia

The **Internet Control Message Protocol (ICMP)** is one of the core protocols of the Internet protocol suite. It is chiefly used by networked computers' operating systems to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached.

ICMP differs in purpose from TCP and UDP in that it is usually *not* used directly by user network applications. One exception is the ping tool, which sends ICMP Echo Request messages (and receives Echo Response messages) to determine whether a host is reachable and how long packets take to get to and from that host.

## Technical Details

The **Internet Control Message Protocol (ICMP)** is part of the Internet protocol suite as defined in RFC 792 (<http://www.ietf.org/rfc/rfc792.txt>). ICMP messages are typically generated in response to errors in IP datagrams (as specified in RFC 1122 (<http://www.ietf.org/rfc/rfc1122.txt>)) or for diagnostic or routing purposes.

The version of ICMP for Internet Protocol version 4 is also known as **ICMPv4**, as it is part of IPv4. IPv6 has an equivalent protocol, **ICMPv6**.

ICMP messages are constructed at the IP layer, usually from a normal IP datagram which has generated an ICMP response. IP encapsulates the appropriate ICMP message with a new IP header (to get the ICMP message back to the original sending host), and transmits the resulting datagram in the usual manner.

For example, every machine (such as intermediate routers) that forwards an IP datagram has to decrement the time to live (TTL) field of the IP header by one; if the TTL reaches 0, an ICMP Time to live exceeded in transit message is sent to the source of the datagram.

Each ICMP message is encapsulated directly within a single IP datagram, and thus, like UDP, ICMP does not guarantee delivery.

Although ICMP messages are contained within standard IP datagrams, ICMP messages are usually processed as a special case distinguished from normal IP processing, rather than processed as a normal sub-protocol of IP. In many cases, it is necessary to inspect the contents of the ICMP message, and deliver the appropriate error message to the application which generated the original IP packet, the one which prompted the sending of the ICMP message.

Many commonly used network utilities are based on ICMP messages. The traceroute command is implemented by transmitting UDP datagrams with specially set IP TTL header fields, and looking for ICMP Time to live exceeded in transit (above) and "Destination unreachable" messages generated in response. The related ping utility is implemented using the ICMP "Echo" and "Echo reply" messages.

### Internet protocol suite

Layer	Protocols
Application	DNS, TLS/SSL, TFTP, FTP, HTTP, IMAP, IRC, NNTP, POP3, SIP, SMTP, SNMP, SSH, TELNET, BitTorrent, RTP, rlogin, ENRP, ...
Transport	TCP, UDP, DCCP, SCTP, IL, RUDP, ...
Network	IP (IPv4, IPv6), ICMP, IGMP, ARP, RARP, ...
Link	Ethernet, Wi-Fi, Token ring, PPP, SLIP, FDDI, ATM, DTM, Frame Relay, SMDS, ...

## Internet Control Message Protocol - Wikipedia, the free encyclopedia

Page 2 of 3

List of permitted control messages (incomplete list):

- 0 - Echo Reply
  - 1 - Reserved
  - 2 - Reserved
  - 3 - Destination Unreachable
  - 4 - Source Quench
  - 5 - Redirect Message
  - 6 - Alternate Host Address
  - 7 - Reserved
  - 8 - Echo Request
  - 9 - Router Advertisement
  - 10 - Router Solicitation
  - 11 - Time Exceeded
  - 12 - Parameter Problem
  - 13 - Timestamp
  - 14 - Timestamp Reply
  - 15 - Information Request
  - 16 - Information Reply
  - 17 - Address Mask Request
  - 18 - Address Mask Reply
  - 19 - Reserved for security
  - 20-29 - Reserved for robustness experiment
  - 30 - Traceroute
  - 31 - Datagram Conversion Error
  - 32 - Mobile Host Redirect
  - 33 - IPv6 Where-Are-You
  - 34 - IPv6 Here-I-Am
  - 35 - Mobile Registration Request
  - 36 - Mobile Registration Reply
  - 37 - Domain Name Request
  - 38 - Domain Name Reply
  - 39 - SKIP Algorithm Discovery Protocol
  - 40 - Photuris, Security failures
  - 41-255 - Reserved
- (Source: IANA ICMP Parameters (<http://www.iana.org/assignments/icmp-parameters>))

## See also

- ICMPv6
- IRDP
- Smurf attack
- TCP

## External links

- RFC 792 (<http://www.ietf.org/rfc/rfc792.txt>), *Internet Control Message Protocol*
- ICMP Sequence Diagram (<http://www.eventhelix.com/RealtimeMantra/Networking/icmp.pdf>)
- RFC 1122 (<http://www.ietf.org/rfc/rfc1122.txt>), *Requirements for Internet Hosts – Communication Layers*

## Internet Control Message Protocol - Wikipedia, the free encyclopedia

Page 3 of 3

Retrieved from "[http://en.wikipedia.org/wiki/Internet\\_Control\\_Message\\_Protocol](http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol)"

Categories: Internet protocols | Internet standards

- This page was last modified 12:46, 30 March 2006.
- All text is available under the terms of the GNU Free Documentation License (see **Copyrights** for details). Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc.
- Privacy policy
- About Wikipedia
- Disclaimers